



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

General Information

Request for TX-RAMP certification can be broken up into various phases, once an assessment has been submitted to DIR, the assessors will evaluate the completed assessment. Upon evaluation completion, the determination of certification is made.

The information within this document will serve as a guide for submitting the required documents, as a part of the Assessment phase.

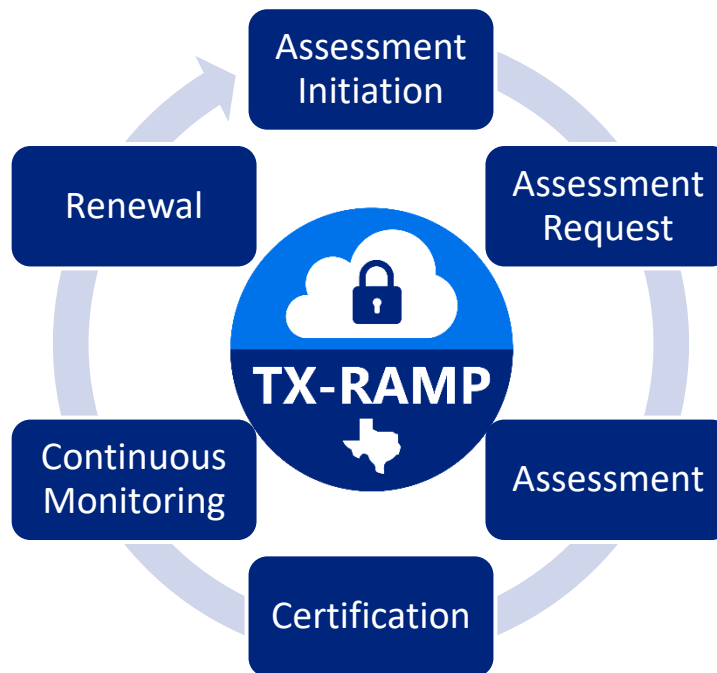


Figure 1. TX-RAMP Certification Lifecycle

Assessment Summary

Certifications will be determined based upon DIR review of an assessment and related documentation ("assessment"). This assessment entails DIR's review of:

- the assessment form and all answers therein submitted by either the vendor or state agency; and
- all documentation submitted to DIR by the vendor either initially or supplementally.

The timeline to complete the assessment is dependent upon vendor responsiveness and completeness of documents. If DIR is required to seek additional documentation or extensive vendor outreach is required, DIR may require more time to certify.



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Completing the Assessment Questionnaire Form

Upon processing the TX-RAMP certification request a TX-RAMP Assessment questionnaire will be sent to the cloud service provider's designated contact to complete. The SPECTRIM Vendor Portal is used to assign and launch assessment questionnaires to vendor contacts to collect assessment responses.

General

The Assessment Questionnaire asks to provide general information about the cloud service for the assessment. For details, see Appendix A. TX-RAMP Assessment – Level 2 Questions.

Documents Required

Provide documentation for the assessment. Documentation requirements may be found in the [TX-RAMP Manual, Appendix B – Required Documentation](#).

Standardizing Documents

- Use a standard format across all documents to assist in ensuring compliance, completeness, consistency, clarity, and conciseness

ABC Services

Scope
The scope of this policy ...

Purpose
The purpose of this policy ...

Roles
This policy applies to ...

Responsibilities

Role(s)	Responsibility
IT Access and Identity Management Team	<ul style="list-style-type: none"> • Provision access to upon receipt of Request Form ...
Etc.	<ul style="list-style-type: none"> • ...

Access Control Policy Page 2 of 5

Figure 2. A standard format can be used for all required documents. This is an example of a header that clearly labels the Scope, Purpose, Roles, and Responsibilities.

- Use of a version history table to assist in confirming proper approvals and review timelines are achieved



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Table 1. Example of a Version History Table. This policy has been reviewed within three years, as per TX-RAMP requirement.

Date	Version Number	Description	Approving Authority
05/01/2019	1.0	Published Access Control Policy	Jim Smith Chief Executive Officer
05/01/2022	2.0	Reviewed and updated Access Control Policy	Jim Smith Chief Executive Officer

TX-RAMP Control Baselines and parameters

- [TX-RAMP Security Control Baselines](#), defines the controls required for TX-RAMP Level 1 and Level 2 certification.
- If uncertain about the policy required for the TX-RAMP assessment questionnaire, the subject matter can be found within the TX-RAMP Security Control Baselines. The Control Baselines can be used as a reference guide to identify the related content within each policy.
- TX-RAMP Parameters - Some controls within the TX-RAMP Security Control Baselines define a minimum requirement level for TX-RAMP compliance. These minimum requirements are located at the bottom of specific controls as "TX-RAMP Parameters".

Table 2. TX-RAMP control, AC-02 (02), the highlighted TX-RAMP parameter requires the information system to automatically remove/disable temporary and emergency accounts after a period of no more than 30 days.

Control ID	Control Description
AC-02 (02)	<p>AC-02 (02) ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].</p> <p>TX-RAMP Parameters: AC-2 (2) [no more than 30 days for temporary and emergency account types]</p>

Required Documentation's Comments

The questionnaire allows the submission of optional comments. Provide additional information or comments within this section, if needed.

Submitting Documents

- Attach applicable document to each section as requested. Do not skip or leave a required document empty.
- If a document covers multiple policies, you may separate the document into multiple documents to cover each policy. However, control requirements must be provided for each submission.



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

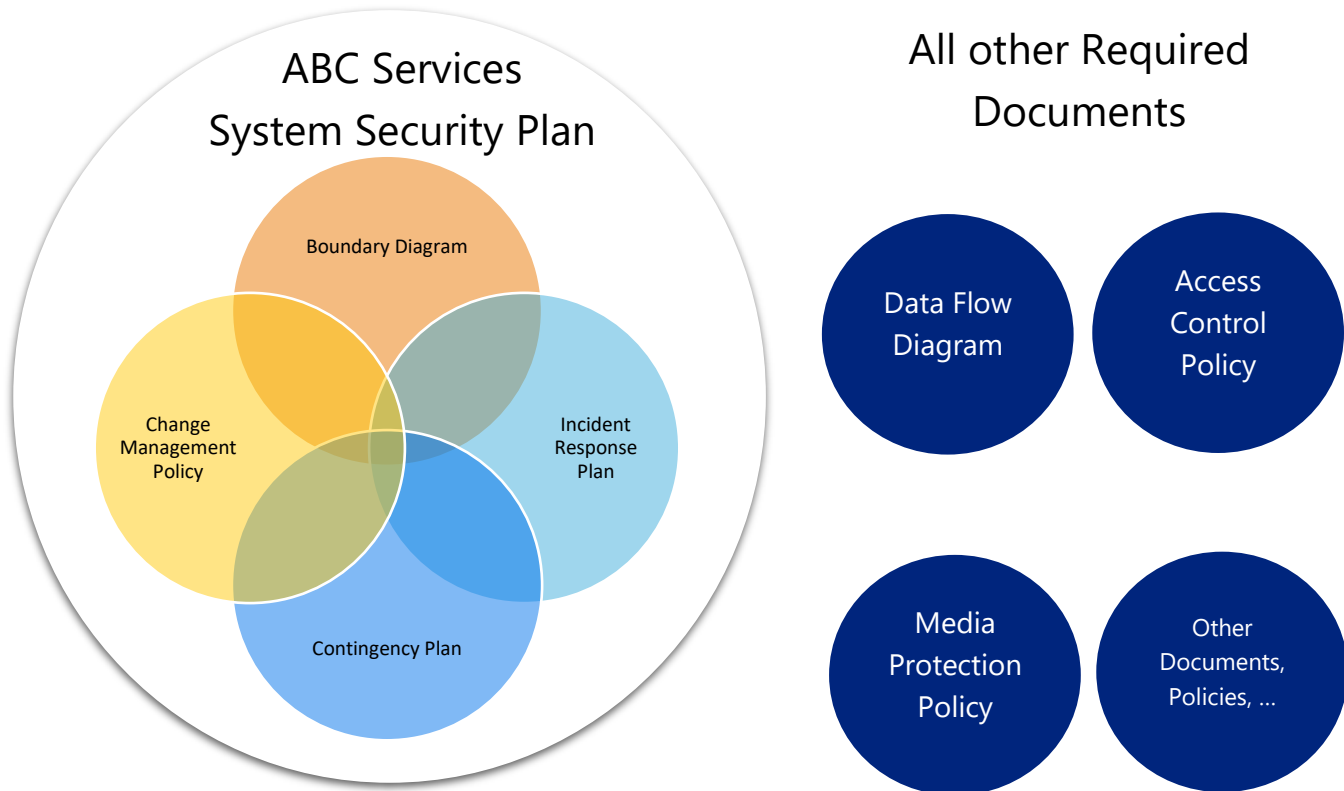


Figure 3. An organization may have other plans or policies found within a central document. In this example, the Change Management Policy, Boundary Diagram, Incident Response Plan, and Contingency Plan are found within ABC Services' System Security Plan (SSP). All other documents required are their own separate plans/policies. Therefore, ABC Services will separate their SSP and attach 5 separate documents to each respective section: the System Security Plan in its entirety for the System Security Plan section, the Change Management Policy for the Configuration Management section, the Boundary Diagram for the Boundary Diagram section, the Incident Response Plan for the Incident Response Plan section, and the Contingent Plan for the Contingency Plan section. ABC Services will then attach all other required documents into their respective sections as well. Additionally, the company can add comments at the bottom of the Required Documents section to provide additional context such as "The System Security Plan contains multiple plans and policies for ABC Services. We have attached the documents from the System Security Plan into each relevant section."

System Security Plan Guidance

- 1) Contains content explained within the respective Control Family (PL | SECURITY PLAN)
- 2) Includes an overview of the Information System, system categorization, and key personnel
- 3) A description of the authorization boundary, a listing of all internal and external types of users and their roles, network architecture, system interconnections, a listing of minimum-security controls and the implementation of each control
- 4) A Control Implementation Summary (CIS) matrix
- 5) A Customer Responsibility Matrix (CRM)



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Note: The [TX-RAMP Security Controls Baseline](#) is a spreadsheet that can be completed as a companion guide for TX-RAMP required documentation submission. The spreadsheet includes both the CIS matrix and CRM for each control.

Control ID	Control Description	Implementation Status	Control Origination	Description of Implementation	Control Inheritance Details (if inherited)	Optional Comments
AC-01	AC-01 ACCESS CONTROL POLICY AND PROCEDURES ... For full details see the TX-RAMP Security Controls Baseline	<input checked="" type="checkbox"/> Implemented <input type="checkbox"/> Partially Implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative Implementation <input type="checkbox"/> Not Implemented <input type="checkbox"/> Not Applicable	<input checked="" type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from Pre-Existing TX-RAMP Certified RAMP Authorization	ABC Services has the Access Control Policy that covers all requirements listed within the Control Description.	N/A	We will also attach the ABC Service Information Security Program that includes additional information for organization-wide policy review cycles.

Table 3. Example of a CIS matrix and CRM found within the TX-RAMP Security Controls Baseline.

- 6) A Rules of Behavior document
- 7) A Separation of Duties Matrix

Control Requirements

Control ID	Document Name(s)	Control Description
PL-02	Security Plan	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops a security plan for the information system that: <ul style="list-style-type: none"> 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency];



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and</p> <p>e. Protects the security plan from unauthorized disclosure and modification.</p> <p>TX-RAMP Parameters: PL-2 (c) [at least annually]</p>
--	--	---

Boundary Diagram/ Authorization Boundary Diagram (ABD) Guidance

A visual representation that:

- Shows system components, services, or devices that reside in the customer's environment may be in boundary, or out of the boundary.
- Lists tools, services, or components that is mentioned in the SSP which should appear on the ABD. (Such as DB, application, server, authentication, production systems, jump boxes, connections, VPN)
- Easy-to-read diagram that includes a legend or labels everything
- Prominent border drawn around all components in the authorization boundary
- All ingress / egress points
- Depict services leveraged from the underlying IaaS/PaaS/SaaS
- Depict all interconnected systems and external services as mentioned in the SSP
- How CSP admins and agency customers access the cloud service
- If applicable, depict components provided by the CSP, and installed on customer devices, as inside the authorization boundary (such as mobile application or clients)
- Shows connections between components within the boundary and to/from external services
- Shows security systems in-place between the boundary and external services and access
- Depicts development/test environment, alternate processing site, and location of backups including the connections and security mechanisms associated with the connections and services
- Show update services (e.g., malware signatures and OS updates) outside the boundary

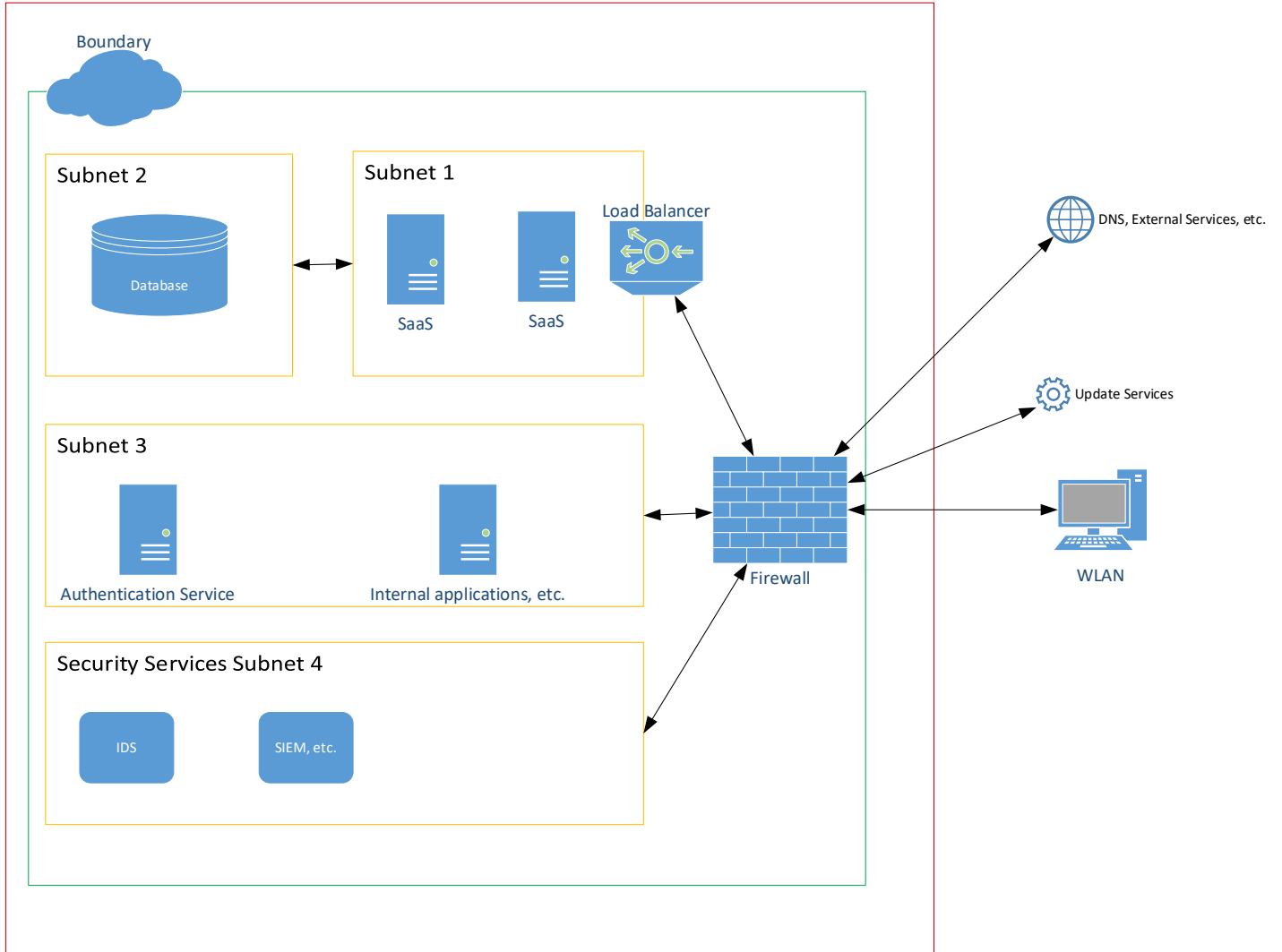


TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Table 4. Example of Boundary Diagram for reference only.




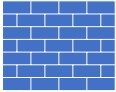




TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Table 5. Example of a legend that provides a description of symbols used within a diagram.

Legend	
Cloud Services for Updates	
Firewall	
Router	
User	 Users

Data Flow Diagram Guidance

A visual representation that:

- Lists authentication mechanism and multi-factor authentication (if applicable)
- Lists external services
- Lists interconnections
- Lists port numbers and protocols used between connections
- Lists sites and backup sites
- Lists the types of data
- Where data is processed, stored, or transmitted
- How data is protected in process, at rest, and when transmitted (cryptographic standards, example TLS v1.2, AES 256, etc.)
- How administrators, staff, customers, and the public access data
- Lists data flow between Development, Test, and Production environments

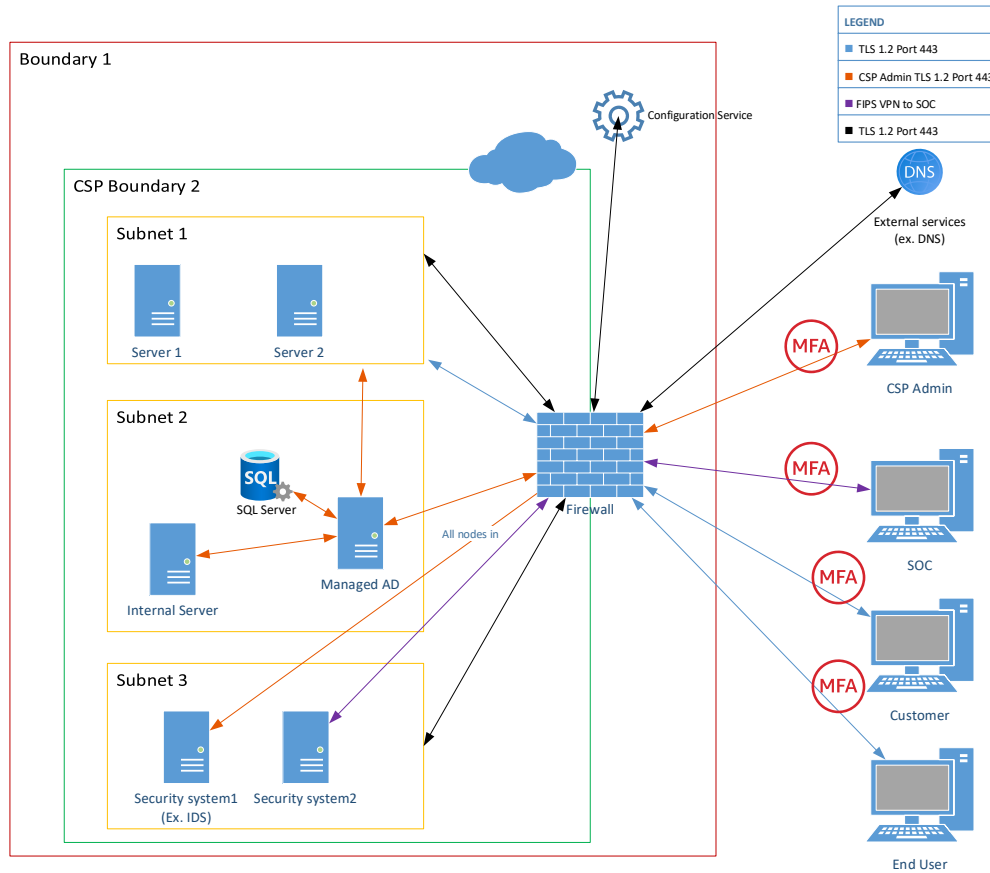


TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Table 6. Example of Data Flow Diagram





TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Incident Response Plan Guidance

A document that:

- Contains content explained within the respective Control Family (IR | INCIDENT RESPONSE)

Control Requirements

Control ID	Document Name(s)	Control Description
IR-08	INCIDENT RESPONSE PLAN	<p>IR-08 INCIDENT RESPONSE PLAN</p> <p>The organization:</p> <ol style="list-style-type: none"> Develops an incident response plan that: <ol style="list-style-type: none"> Provides the organization with a roadmap for implementing its incident response capability; Describes the structure and organization of the incident response capability; Provides a high-level approach for how the incident response capability fits into the overall organization; Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; Defines reportable incidents; Provides metrics for measuring the incident response capability within the organization; Defines the resources and management support needed to effectively maintain and mature an incident response capability; and Is reviewed and approved by [Assignment: organization-defined personnel or roles]; Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; Reviews the incident response plan [Assignment: organization-defined frequency]; Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and Protects the incident response plan from unauthorized disclosure and modification. <p>TX-RAMP Parameters:</p> <p>The service provider defines a list of incident response personnel (identified by name and/or by role) and</p>



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		organizational elements. The incident response list includes designated contracting agency personnel.
--	--	---



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Information System Contingency Plan Guidance

A document that:

- Contains content explained within the respective Control Family (CP | CONTINGENCY PLAN)

Control Requirements

Control ID	Document Name(s)	Control Description
CP-02	CONTINGENCY PLAN	<p>CP-02 CONTINGENCY PLAN</p> <p>The organization:</p> <ol style="list-style-type: none"> Develops a contingency plan for the information system that: <ol style="list-style-type: none"> Identifies essential missions and business functions and associated contingency requirements; Provides recovery objectives, restoration priorities, and metrics; Addresses contingency roles, responsibilities, assigned individuals with contact information; Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and Is reviewed and approved by [Assignment: organization-defined personnel or roles]; Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; Coordinates contingency planning activities with incident handling activities; Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and Protects the contingency plan from unauthorized disclosure and modification. <p>TX-RAMP Parameters: CP-2 (d) [at least annually]</p>



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Configuration Management Plan Guidance

A document that:

- Contains content explained within the respective Control Family (CM | CONFIGURATION MANAGEMENT)

Control Requirements

Control ID	Document Name(s)	Control Description
CM-09	CONFIGURATION MANAGEMENT PLAN	<p>CM-09 CONFIGURATION MANAGEMENT PLAN</p> <p>The organization develops, documents, and implements a configuration management plan for the information system that:</p> <ul style="list-style-type: none"> a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.

Policy – Access Control (AC)

Control Requirements

Control ID	Document Name(s)	Control Description
AC-01	ACCESS CONTROL POLICY AND PROCEDURES	<p>AC-01 ACCESS CONTROL POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p>



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		AC-1 (b) (1) [at least every 3 years] AC-1 (b) (2) [at least annually]
--	--	---

Policy – Awareness and Training (AT)

Control Requirements

Control ID	Document Name(s)	Control Description
AT-01	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	<p>AT-01 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters: AT-1 (b) (1) [at least every 3 years] AT-1 (b) (2) [at least annually]</p>

Policy – Audit and Accountability (AU)

Control Requirements

Control ID	Document Name(s)	Control Description
AU-01	AUDIT AND ACCOUNTABILITY POLICY AND	<p>AU-01 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters: AU-1 (b) (1) [at least every 3 years] AU-1 (b) (2) [at least annually]</p>
--	--	---

Policy – Security Assessment and Authorization (CA)

Control Requirements

Control ID	Document Name(s)	Control Description
CA-01	SECURITY ASSESSMENT AND AUTHORIZATION	<p>CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES</p> <p>The organization:</p> <ol style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ol style="list-style-type: none"> 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: <ol style="list-style-type: none"> 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters: CA-1 (b) (1) [at least every 3 years] CA-1 (b) (2) [at least annually]</p>

Policy - Configuration Management (CM)

Control Requirements

Control ID	Document Name(s)	Control Description
CM-01	CONFIGURATION MANAGEMENT POLICY AND	<p>CM-01 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES</p> <p>The organization:</p> <ol style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment:



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>CM-1 (b) (1) [at least every 3 years]</p> <p>CM-1 (b) (2) [at least annually]</p>
--	--	---



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Policy - Contingency Planning (CP)

Control Requirements

Control ID	Document Name(s)	Control Description
CP-01	CONTINGENCY PLANNING POLICY AND	<p>CP-01 CONTINGENCY PLANNING POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters: CP-1 (b)(1) [at least every 3 years] CP-1 (b)(2) [at least annually]</p>

Policy - Identification and Authentication (IA)

Control Requirements

Control ID	Document Name(s)	Control Description
IA-01	IDENTIFICATION AND AUTHENTICATION POLICY AND	<p>IA-01 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Identification and authentication policy [Assignment:



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>organization-defined frequency]; and</p> <p>2. Identification and authentication procedures [Assignment: organization-defined frequency].</p> <p>TX-RAMP Parameters:</p> <p>IA-1 (b) (1) [at least every 3 years]</p> <p>IA-1 (b) (2) [at least annually]</p>
--	--	--

Policy - Incident Response (IR)

Control Requirements

Control ID	Document Name(s)	Control Description
IR-01	INCIDENT RESPONSE POLICY AND PROCEDURES	<p>IR-01 INCIDENT RESPONSE POLICY AND PROCEDURES</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>IR-1 (b) (1) [at least every 3 years]</p> <p>IR-1 (b) (2) [at least annually]</p>

Policy - Maintenance (MA)

Control Requirements

Control ID	Document Name(s)	Control Description
MA-01	SYSTEM MAINTENANCE POLICY AND PROCEDURES	<p>MA-01 SYSTEM MAINTENANCE POLICY AND PROCEDURES</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>maintenance policy and associated system maintenance controls; and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>MA-1 (b) (1) [at least every 3 years]</p> <p>MA-1 (b) (2) [at least annually]</p>
--	--	---

Policy - Media Protection (MP)

Control Requirements

Control ID	Document Name(s)	Control Description
MP-01	MEDIA PROTECTION POLICY AND PROCEDURES	<p>MP-01 MEDIA PROTECTION POLICY AND PROCEDURES</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>MP-1 (b) (1) [at least every 3 years]</p> <p>MP-1 (b) (2) [at least annually]</p>

Policy - Physical and Environmental Protection (PE)

Control Requirements

Control ID	Document Name(s)	Control Description
PE-01	PHYSICAL AND ENVIRONMENTAL PROTECTION	<p>PE-01 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment:</p>



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>PE-1 (b) (1) [at least every 3 years]</p> <p>PE-1 (b) (2) [at least annually]</p>
--	--	--

Policy - Planning (PL)

Control Requirements

Control ID	Document Name(s)	Control Description
PL-01	SECURITY PLANNING POLICY AND PROCEDURES	<p>PL-01 SECURITY PLANNING POLICY AND PROCEDURES</p> <p>The organization:</p> <ol style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ol style="list-style-type: none"> 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and <ol style="list-style-type: none"> b. Reviews and updates the current: <ol style="list-style-type: none"> 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>PL-1 (b) (1) [at least every 3 years]</p> <p>PL-1 (b) (2) [at least annually]</p>

Policy - Personnel Security (PS)



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Control Requirements

Control ID	Document Name(s)	Control Description
PS-01	PERSONNEL SECURITY POLICY AND PROCEDURES	<p>PS-01 PERSONNEL SECURITY POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters: PS-1 (b) (1) [at least every 3 years] PS-1 (b) (2) [at least annually]</p>

Policy - Risk Assessment (RA)

Control Requirements

Control ID	Document Name(s)	Control Description
RA-01	RISK ASSESSMENT POLICY AND PROCEDURES	<p>RA-01 RISK ASSESSMENT POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters: RA-1 (b) (1) [at least every 3 years] RA-1 (b) (2) [at least annually]</p>



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Policy - System and Services Acquisition (SA)

Control Requirements

Control ID	Document Name(s)	Control Description
SA-01	SYSTEM AND SERVICES ACQUISITION POLICY AND	<p>SA-01 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency]. <p>TX-RAMP Parameters:</p> <p>SA-1 (b) (1) [at least every 3 years]</p> <p>SA-1 (b) (2) [at least annually]</p>

Policy - System and Communications Protection (SC)

Control Requirements

Control ID	Document Name(s)	Control Description
SC-01	SYSTEM AND COMMUNICATIONS PROTECTION	<p>SC-01 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES</p> <p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current:



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

		<p>1. System and communications protection policy [Assignment: organization-defined frequency]; and</p> <p>2. System and communications protection procedures [Assignment: organization-defined frequency].</p> <p>TX-RAMP Parameters:</p> <p>SC-1 (b) (1) [at least every 3 years]</p> <p>SC-1 (b) (2) [at least annually]</p>
--	--	---

Policy - System and Information Integrity (SI)

Control Requirements

Control ID	Document Name(s)	Control Description
SI-01	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	<p>SI-01 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES</p> <p>The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <p>1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and</p> <p>b. Reviews and updates the current:</p> <p>1. System and information integrity policy [Assignment: organization-defined frequency]; and</p> <p>2. System and information integrity procedures [Assignment: organization-defined frequency].</p> <p>TX-RAMP Parameters:</p> <p>SI-1 (b) (1) [at least every 3 years]</p> <p>SI-1 (b) (2) [at least annually]</p>



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Responding To Questions Within Each Control Family

The questionnaire separates the questions by each Control Family. Questions are derived from the TX-RAMP Security Controls Baseline documentation for the assessment. Details found may be found in the [TX-RAMP Manual, Appendix A - TX-RAMP Control Baselines](#).

TX-RAMP Level	Number of Controls/Enhancements Assessed
Level 1	124
Level 2	325

CONTROL FAMILY	TX-RAMP LEVEL 1	TX-RAMP LEVEL 2
ACCESS CONTROL	11	43
AUDIT AND ACCOUNTABILITY	10	19
AWARENESS AND TRAINING	4	5
CONFIGURATION MANAGEMENT	8	27
CONTINGENCY PLANNING	6	24
IDENTIFICATION AND AUTHENTICATION	15	27
INCIDENT RESPONSE	8	18
MAINTENANCE	4	11
MEDIA PROTECTION	4	10
PERSONNEL SECURITY	8	8
PHYSICAL AND ENVIRONMENTAL PROTECTION	9	20
PLANNING	3	6
RISK ASSESSMENT	4	10
SECURITY ASSESSMENT AND AUTHORIZATION	8	15
SYSTEM AND COMMUNICATIONS PROTECTION	8	32
SYSTEM AND INFORMATION INTEGRITY	7	28
SYSTEM AND SERVICES ACQUISITION	7	22
TOTAL	124	325

Figure 4. Applicable Controls per Control Family



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Guidance for Choosing a Response Option

The questionnaire asks if TX-RAMP controls are being met. As a submitter, providing responses will help reduce the challenges evaluators face when reviewing and processing the completed Assessment questionnaires.

Guidance for Responding to the Questionnaire

- Answer questions from the perspective of the Cloud Service Provider and not the Customer
 - Use the free text fields at the end of each control family to provide additional context
 - If responding with a "No" please:
 - Identify if there are Customer specific requirements that must be met to address the lack of security control implementation
 - Provide a brief description as to why control is not met within the comments section
 - How the lack of this control may affect the agency customer
 - The compensating controls
 - If there is a remediation plan
 - The target date of remediation
 - Supply a Plan of Action and Milestones (POAM) to provide a structured list of controls not met and to illustrate the next steps
- Resource:** [FedRAMP Plan of Action and Milestones \(POA&M\) Template](#)
- If responding with a "N/A" please:
 - Provide a narrative about customer control responsibilities
 - Reference Customer Responsibility Matrix (CRM), if applicable



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Table 7. Example of a POAM that illustrates a POAM to remediate controls that are not in effect.

Control #	Control Description	Risk Statement	Compensatin g Control	Point of Contact	Remediation Plan	Milestones	Scheduled Completion Date	Completion Status	Comments
AT-02 (02)	AT-02 (02) SECURITY AWARENESS INSIDER THREAT The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	Lack of awareness regarding recognizing and reporting potential indicators of insider threat may result in longer durations of system compromise and unauthorized access.	Employees are trained on external threats, such as phishing, and know to report potential security incidents to IT.	John Smith	Security Awareness training will be updated to include indicators of insider threats.	5/1/2022 Draft updated training material.	1/1/2023	Open	N/A



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Resources

Texas Risk and Authorization Management Program (TX-RAMP) website

<https://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp>

TX-RAMP Overview for Vendors (PDF)

<https://dir.texas.gov/sites/default/files/2022-01/TX-RAMP%20Overview%20Webinar%20For%20Vendors.Update.pdf>

FedRAMP Resources and Templates

<https://www.fedramp.gov/documents-templates/>

StateRAMP Resources and Templates

<https://stateramp.org/templates-resources/>

For TX-RAMP Assistance and Questions

Contact TX-RAMP@dir.texas.gov



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Version History

Date	Version Number	Description
06/21/2022	1.0	Published document



TX-RAMP Vendor Guide:

Level 1 and 2 Assessment Questionnaire Required Documents

June 2022

Appendix A. TX-RAMP Assessment – Level 2 Questions



TX-RAMP
Assessment - Level 2